Република Србија
Аутономна Покрајина Војводина
Општина Бачка Топола
ОПШТИНСКА УПРАВА
Број : службено
Дана: 06.02.2024. године
Бачка Топола

Министарство унутрашњих послова
Високотехнолошки криминал
Београд
vtk@mup.gov.rs

Допис: Извештај о Ransomver нападу дана 05.04.2024. године

Дана 05.02.2024 године ујутро у 7 сати смо приметили напад на наш рачунар за Евиденцију улаза и излаза радника Општинске управе. На екрану се појавила порука, и јасно писало да се десио Ransomver напад. Порука је у прилогу бр 1. На том рачунару се налазио само програм Мега за евиденцију радника. Сваки фајл који се налази на том рачунару је блокиран и има екстензију .exe, Прилог бр 2. На десктопу је такође сваки Shortcut блокиран, приликом отварање појави се иста порука о обавештењу о нападу, Прилог бр 3. На рачунару је био инсталиран програм за даљинско приступање Anydesk, који је коришћен од стране програмера. Anydesk је подешен са приступном шифром, стим је Мега по потреби имала неограничен приступ рачунару. На рачунару је мапиран фолдер према њиховом серверу. Према подацима последњих измена фајлова напад се десио око 20 сати дана 04.02.2024. године, Прилог бр 4. На серверу програма Мега се десио мало касније, после 21 часова.

На серверу је такође био инсталиран Anydesk програм, преко које су програмери фирме Мега имали приступ и радили одржавање. На серверу смо такође исте промене приметили. Сваки фајл је блокиран и добио екстензију .exe. Оперативни систем ради на оба рачунара као и основни програми (File Explorer, Total Commander). На овом рачунару се налази база података системског програма Мега. База података је исто блокирана као и сви фајлови које су на том рачунару. На овом рачунару је мапиран фолдер са нашег домен сервера.

На домен серверу су оштећени фајлови који су се налазили на тој партицији са којег је подељен фолдер према Мега серверу. На тој партицији смо имали заједничке фолдере корисника, у највећем случају word, excel, pdf и jpg документа, која су после напада исто добили екстензију .exe. На рачунару остале партиције са документима и сам оперативни систем није оштећен.

Рачунаре смо одмах искључили из мреже. Домен сервер је после чишћења и враћања backup података укључен у нормалан рад. Мега сервер је ван функције, чекамо од програмерске куће инструкције за даљи приступ.

Контакт особа је Богларка Чеварушић, Руководилац групе за информатику, број телефона 063658755, мејл адреса webmaster@btopola.org.rs .

У Бачкој Тополи, 06.02.2024.г.

Начелник Општинске управе

Петер Седлар